IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
WESTERN DIVISION

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

In the Matter of the Search of a Western Digital Hard Drive Model #4808A, Serial Number WCAU40312890, in the Custody of FBI Memphis

CASE NO: 17-SW-129

I David E. Palmer being duly sworn depose and say:

I am a Special Agent, Federal Bureau of Investigations ,and have reason to believe that on the property or premises known as

(SEE ATTACHMENT A which is attached hereto and fully incorporated herein by reference)

in the WESTERN District of TENNESSEE there is now located certain property, namely,

(SEE ATTACHMENT B which is attached hereto and fully incorporated herein by reference)

which is (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of crime; (3) property designed or intended for use and which is or has been used as the means of committing a criminal offense, concerning a violation of Title 42 U.S.C. Section 1320d-6.

The facts to support a finding of Probable Cause are as follows:

(SEE ATTACHMENT C: AFFIDAVIT OF DAVID E. PALMER in support of Application For Search Warrant, which is attached hereto and fully incorporated herein by reference)

Continued on the attached sheet and made a part hereof X Yes __No

DAVID E. PALMER - Affiant

Pursuant to Federal Rule of Criminal Procedure 41(d)(3), the undersigned judicial officer has on this date considered information communicated by [ ] telephone or [ ] other reliable electronic means or [✓] both, in reviewing and deciding whether to issue a search warrant. In doing so, this judicial officer has placed the affiant under oath and has confirmed by speaking personally with the affiant on the telephone [✓] that the signatures on the search warrant application and affidavit are those of the affiant or [ ] that the affiant has authorized the placement of the affiant's signatures on the application and affidavit, the documents received by the judicial officer are a correct and complete copy of the documents submitted by the affiant, and the information contained in the search warrant application and affidavit are true and correct to the best of the affiant's knowledge.

Sworn to and subscribed before me by telephone this 21st day of June 2017.

Charmiane G. Claxton, Magistrate Judge
Name & Title of Judicial Officer

Signature of Judicial Officer

IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TENNESSEE

STATE OF TENNESSEE	**Case No.** 17-SW-129
COUNTY OF SHELBY	**Filed Under Seal**

AFFIDAVIT

I, David E. Palmer, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January 11, 2015. I am currently assigned to the FBI Field Office in Memphis, Tennessee. I have received training in criminal investigations and in investigating and prosecuting cyber- and computer-related offenses.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the examination of property – one electronic device – which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

3. Your Affiant is conducting an investigation into certain activities of the subject Jeffrey R. Luke (Luke), in violation of Title 18, United States Code (U.S.C.) Sections 1030(a)(2)(C), and (b)(2)(B) (Fraud and related activity in connection with computers) and Title 42, U.S.C. Section 1320d-6 (Obtaining individually identifiable health information on an individual).

4. The following information was obtained through observations and conversations of your Affiant personally, through the assistance of other law enforcement agents and agencies, including their reports, and through other sources specifically named in this affidavit. Since this affidavit is being submitted for the limited purpose of securing a search

warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of violations of Title 18, U.S.C. Sections 1030 and Title 42, U.S.C. Section 1320d-6, and that the electronic device identified in **Attachment A** contains evidence of said violations. The evidence believed to be located on the electronic devices identified in **Attachment A** is listed in **Attachment B**, both of which are incorporated by reference as if fully set for herein.

STATUTORY AUTHORITY

5. Section 1320d-6 of Title 42 provides that:

(a) A person who knowingly and in violation of this part –

(1) uses or causes to be used a unique health identifier;

(2) obtains individually identifiable health information relating to an individual; or

(3) discloses individually identifiable health information to another person,

...shall be guilty of an offense against the United States.

6. Section 1030(a) of Title 18 provides, in pertinent part, that whoever:

(a)(2)(C) intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer;

(a)(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value;

(a)(5)(C) intentionally accesses a protected computer without authorization, and as a result of such conduct causes damage and loss;

...shall be guilty of an offense against the United States.

RELEVANT STATUTORY DEFINITIONS AND TERMS

7. The term "**individually identifiable health information**" is defined as patient information protected by the Health Insurance Portability and Accountability Act (HIPPA) of 1996. HIPPA provides data privacy and security provisions for safeguarding medical information.

(a) A person (including an employee or other individual) shall be considered to have obtained or disclosed individually identifiable health information in violation of 42 U.S.C. § 1320d-6 if the information is maintained by a covered entity (as defined in the HIPPA privacy regulation described in section 1320d-9 (b)(3) of this title) and the individual obtained or disclosed such information without authorization.

8. The term "**computer**," as used herein, is defined pursuant to Title 18, U.S. Code § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

9. The term "**protected computer**," as used herein, means a computer which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce of the United States.

10. The term "**exceeds authorized access**," as used herein, means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled to obtain or so alter.

DGP

11. The term "**damage**," as used herein, means any impairment to the integrity or availability of data, a program, a system, or information.

12. The term "**loss**," as used herein, means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.

13. The terms "**records**," "**documents**", and "**materials**" include all information recorded in any form, visual or aural, hard copy or digital, including the originals and all non-identical copies thereof, whether different from the original by reason of any notation made on such copies or otherwise, including, but not limited to the following:

(a) Written or printed matter of any kind, correspondence, memoranda, notes, diaries, statistics, letters, telephone toll records, telegrams, contracts, reports, checks, statements, receipts, returns, summaries, pamphlets, books, ledgers, journals, registers, records, vouchers, slips, bills, calendars, pads, notebooks, files, logs, lists, bulletins, credit materials, databases, teletypes, telefaxes, invoices, worksheets;

(b) Graphic records or representations, photographs, slides, drawings, designs, graphs, charts, pictures, sketches, images, films, videotapes, and aural recordings or representations, tapes, records, discs.

14. The terms "records," "documents" and "materials" include all of the foregoing in whatever form and by whatever means the records, documents or materials, their drafts or their modifications, may have been created or stored, including (but not limited to) any handmade form (such as writing, drawing, painting, with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides,

DJP

negatives, videotapes, motion pictures, photocopies); and mechanical form (such as tape recordings, cassettes, compact discs, or any information on an electronic or magnetic storage device such as floppy diskettes, hard disks, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives or electronic notebooks, as well as printouts or readouts from any magnetic storage device).

PROBABLE CAUSE

15. On March 8, 2017, the Federal Bureau of Investigation (FBI), Memphis Field Office, received a complaint via the Internet Crime Complaint Center (IC3) from Transformations Autism Treatment Center (TATC) regarding an apparent computer intrusion at the TATC office at 6761 Stage Road, Bartlett, Tennessee.

16. TATC is an applied behavior analysis and treatment center located in Bartlett, Tennessee. The facility primarily treats patients with Autism disorder and is defined by HIPPA as a medical facility.

17. TATC owner Tracy Palm reported on March 31, 2017, that TATC stores HIPPA-protected patient information such as names, dates of birth (DoB), social security numbers, addresses, medical information, and doctors' referrals on a Google Drive account. Google Drive is a file storage and synchronization service that allows individual or business users to set up an account and store files in the "cloud," synchronize files across devices, and share files. "Cloud" or "cloud storage," as used herein, is a mechanism in which files can be saved to an off-site storage system maintained by a third-party—here, Google—where files are saved to a remote database instead of the (user's) computer's hard drive. The

Internet provides the connection between the user's computer and the database for saving and retrieving the files.

18. On March 7, 2017, Palm discovered that all TATC patient files from 2006 to present had been removed from their location on the TATC Google Drive account and placed into a new folder titled "TATC Google Drive" that had not been created by any currently employed staff members. Palm contacted Wade Gillis, an Information Technology (IT) contractor who provides computer services to TATC, and requested he look into the situation.

19. Your Affiant is aware that servers can contain a great deal of information about the devices used to access the server and internet protocol (IP) addresses through which those devices gained access. Simply stated, IP addresses serve a function similar to that of street addresses for residences. IP addresses ensure that internet traffic is routed to the computer or device that is requesting it, rather than to some other device at some other location.

20. Gillis began an internal investigation by reviewing logs from TATC's Google Drive from October 3, 2016 through March 8, 2017. The email account lbtoffice@transformingautism.com, an email account used by TATC employees to access the Google drive account, showed unexplained activity beginning on March 1st. After eliminating known sources, such as computers inside TATC, Gillis determined that the email account had been accessed by external IP address 75.66.167.39 on March 1, 2017. Palm stated that by accessing the TATC Google Drive account using compromised email account, the intruder was able to read and access individually identifiable health information on all of TATC's patients.

DLP

21. Gillis conducted a search for other communications coming from the IP address 75.66.167.39, and learned that on March 3, 2017, the TATC Google Drive was accessed using the external IP address and an "invitation to collaborate" email was sent from lbtoffice@transformingautism.com to jeffrluke@gmail.com for the newly created folder. The email address jeffrluke@gmail.com also displayed Google username "Jeffrey Luke". The intruder then added email address jeffrluke@gmail.com to the access list for the new folder. An invitation to collaborate is a mechanism by which a party not already authorized to access a file or account can be granted access. The invitation is sent via email, and generally contains a link to the subject file. Gillis subsequently changed the passwords for the TATC Google Drive accounts and removed access for jeffrluke@gmail.com. Gillis continued to monitor the TATC accounts after the passwords were changed and discovered that between March 7th and 8th, the intruder utilizing IP address 75.66.167.39 made approximately 13 additional unsuccessful attempts to log into the TATC Google Drive account.

22. Palm explained to your Affiant that Jeffrey Luke is the name of a former employee of TATC. Palm stated he was fired from TATC on February 16, 2017. Luke was employed as a Behavior Analyst at TATC where he would work directly with patients and bill the patients and/or their insurance for his time. In preparation for firing Luke, the staff at TATC changed the Google Drive access passwords on February 13, 2017 and removed Luke's access to the system.

23. On March 31, 2017, your Affiant along with Bartlett Police detective Beky Anderson interviewed Palm and Gillis at the TATC office, 6761 Stage Rd, Bartlett, TN. During the

interview, Gillis provided Agents with a log file titled "AuditReport-20170331-1113" showing all login and logout activity on the TATC Google Drive account from October 3, 2016 to Present. Your Affiants review of the log files revealed the following events involving IP address 75.66.167.39:

Event Description	IP Address	Date
LBT Office logged in	75.66.167.39	October 18 2016 2:14:24 AM GMT
LBT Office logged in	75.66.167.39	February 14 2017 9:29:57 PM GMT
LBT Office logged out	75.66.167.39	March 3 2017 7:47:15 PM GMT
LBT Office logged in	75.66.167.39	March 3 2017 7:41:26 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 3 2017 7:41:17 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 3 2017 7:41:11 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 7 2017 11:21:21 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 7 2017 11:21:13 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 7 2017 11:15:34 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 7 2017 11:15:29 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 7 2017 11:15:22 PM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 8:47:00 AM GMT

LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 3:13:37 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 3:13:29 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 3:13:20 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 1:15:54 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 1:15:45 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 1:15:35 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 1:15:29 AM GMT
LBT Office failed to login because of Invalid Password	75.66.167.39	March 8 2017 1:15:21 AM GMT

Gillis also provided Agents with a log file titled "LogSearchResults-20170331-1812" which contained a records of the "Invitation to collaborate" emails generated from the TATC Google Drive. Your Affiants review of this log file revealed the following item:

Start date	**End date**	**Subject**	**Direction**	**Recipient Address**	**Event Status**	**Event target IP address**
2017/03/03 19:47:00 UTC	2017/03/03 19:47:00 UTC	LBT Office - Invitation to collaborate	Sent	jeffrluke@gmail.com	DELIVERED	75.66.167.39

23. Using publically-available databases, your Affiant determined that the IP address 75.66.167.39 was associated with Comcast, for assignment to its internet service customers. Your affiant sent a subpoena to Comcast, requesting subscriber information for the Comcast customer assigned IP address 75.66.167.39 on March 3, 2017, at 07:41:26 PM GMT.

25. On April 5, 2017, in response to the subpoena, Comcast provided subscriber and identifying information for the IP address 75.66.167.39 that was assigned on March 3, 2017, at 07:41:26 PM GMT. The identifying information indicated the subscriber name was "NICOLE SHAY" with a service address of "853 Meadow Vale Dr, Collierville, TN 380171352". The email user ID's for the account were nickishay@comcast.net and jeffrluke@comcast.net.

26. TATC provided FBI Memphis Agents with Jeffrey Luke's Application for employment with TATC dated February 8, 2015. In the application, Luke listed his current address as "853 Meadow Vale Dr., Collierville, TN 38017".

27. On April 10, 2017, your Affiant conducted a query of the Shelby County, TN Assessor of Property database located at www.assessor.shelby.tn.us. Database records indicate that the property at 853 Meadow Vale Dr, Collierville, TN is owned by Jeffrey R Luke and Nicole L Shay.

28. On April 18, 2017, FBI Memphis Field Office executed Federal Search Warrant 17-SW-068 at the residence located at 853 Meadowvale Ln, Collierville, Tennessee. The search warrant was executed based on probable cause that Jeffrey Luke, a resident of the referenced address, violated Title 18, United States Code, Section 1030, involving unauthorized access to the computer network at Transformations Autism Treatment

Center, and HIPPA violations. During the search of the residence multiple electronic devices were seized as evidence, including a Western Digital hard drive Model #4808A, Serial Number WCAU40312890. A review of the contents of the hard drive commenced on April 20, 2017, with imaging of the hard drive. "Imaging" is the process of creating an exact copy of digital evidence. The image itself will then be searched for evidence responsive to the search warrant, protecting the original evidence from alteration or damage. Initial review of the contents began on or about April 21, 2017.

29. On June 20, 2017, Agents from FBI Memphis continued their review of the contents of the hard drive seized from Luke pursuant to search warrant 17-SW-068. While searching the devices for the items listed in Attachment B of the warrant, Agents also found evidence of other criminal activity, specifically, indication that the drive contained files related to a separate medical treatment facility. On the Western Digital hard drive Model #4808A, Serial Number WCAU40312890, there was a folder titled "BCS stuff." Within that folder were subfolders titled "employee folders" which contained the names of individuals, including Luke. Within Luke's subfolder were multiple documents including one titled "Client Information (New2015).xlsx" with a timestamped "date modified" of March 26, 2017. Analysis of this file showed that it was an Excel Spreadsheet. Also within the folder were several documents with titles that indicated Luke had been employed by BCS, which was identified as Behavioral and Counseling Services (BCS), LLC, in Somerville, Tennessee.

30. On June 20, 2017, your Affiant interviewed Dr. Michael Rohr, owner of Behavioral and Counseling Services, LLC. Rohr confirmed that Luke was employed as a behavioral

counselor by BCS from late 2015 until approximately the fall of 2016. Luke's responsibilities included working with patients and maintaining a full client case load. Rohr stated that during Luke's employment he was given access to a Dropbox account with patient files that were to be accessed in "real time" during his sessions with each patient. Rohr also stated that Luke's employment contract with BCS prohibited him from downloading or saving any documents, including client information, to his computer or any other hard drive.

TECHNICAL TERMS

31. Based on my training and experience, I use the following technical terms to convey the following meanings:

32. **IP Address**: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 21.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

33. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices

communicating with each other are in the same state.

CONCLUSION

34. Based on the foregoing, your Affiant asserts that there is probable cause to believe Luke has violated 42 U.S.C. § 1320d-6 by obtaining individually identifiable health information relating to individuals associated with or treated through Behavioral and Counseling Services, and requests that the Court issue the proposed search warrant for the electronic device identified in Attachment A, which is currently in the possession of the FBI.

AND FURTHER, AFFIANT SAITH NOT.

David E. Palmer - AFFIANT
Special Agent,
Federal Bureau of Investigation

Sworn to and subscribed before me by telephone this 21st day of June, 2017.

21 June 2017
DATE

CHARMIANE G. CLAXTON
UNITED STATES MAGISTRATE JUDGE

Attachment A

Description of ITEM to be searched:

A Western Digital Hard Drive, Model **#4808A, Serial Number WCAU40312890,** presently in the custody of the Federal Bureau of Investigation, Memphis, 225 North Humphreys Blvd., Memphis, Tennessee.

DEP

ATTACHMENT B

ITEMS TO BE SEIZED

Any electronic data (of any type), including but not limited to registry artifacts, images, video recordings, audio recordings, documents, databases, spreadsheets, electronic mail, instant messages, "chats", voicemail, or other communications, contained with the device which:

- Identifies the owner and user of said device and the files contained therein;
- Identifies the manner in which said device was used;
- Contains any image, description, record, receipt, communication, or other file or documents related to violations of Title 18, United States Code, Section 1030 (Fraud and Related Activity in Connection with Computers) or Title 42, United States Code, Section 1320d-6 (Obtaining Individually Identifiable Health Information), as well as aiding and abetting or conspiracy to commit same;
- Specifically related to BCS a.k.a. Behavioral and Counseling Services, LLC